Technical Issues Raised By CyberSecurity Policy

Sandy Merola

January 17, 2001

Outline

- DOE-wide community policies (directives)
- Minimizing the number of Future Poor Policies
- Policy can bring clarity to and motivate:
  - Protection, Detection, Reaction
  - associated technologies
- Deliverable for this session:

  Identify CyberSecurity technologies motivated by Appropriate Policy
- Deliverable for this workshop:

  identify Technologies motivating DOE R&D

DOE-wide Community Policies

- Cyber Security Architecture
- 205.1 Unclassified Computer Security Program
- 205.2 Foreign National Access to Cyber Systems
- 205.3 Password Generation
- 206.1 Electronic Mail Analysis Capability
- 470.2 Independent Oversight and Performance Assurance
- CyberSecurity Performance Compliance checklist

Minimizing the number of Future Poor Policies

Improved cybersecurity practices, in the context of mission, should result in reduced motivation for half-baked policies, by:

- **Reducing the overall risk to the enterprise**
- **Eliminating specific weaknesses for which reactive policies are sometimes instituted**
- **Improving ability to demonstrate cost/benefit approaches with agreement on acceptable risks**
- **Demonstrating Success via a joint policy/technology approach**

(if the above is too optimistic,
we reaffirm our efforts to achieve valued-added policies,
but not generate technology to support poor policy)

Guidelines For Good Policy

Good Policy

- Is Driven by mission
- Is inherent to a prudent cybersecurity program
- Results from identified specific threats/vulnerabilities and a cost/benefit approach to reduce risk
- Is driver for and a partner with Technology
- Is thin but durable, specifying outcomes
- Implementation can be verified
- Is understood, in motivation and implementation, by those who must comply with them

Connecting research funding to DOE needed policies helps motivate/secure funding

Policy driving Technology

Protection:

- Authentication
- Configuration Management
- Firewalls, VPN
- Filtering

Detection:

- Host Based intrusion detection
- Network Based intrusion detection
- Electronic Mail Analysis Capability

Response:

- Incident Response
- Activity blocking
- Disaster Planning
- Incident Reporting & Evidence Collection
- Forensics, Secure Auditing

Needed Interactions between policies and technologists

1. **Develop Security Models that support widely distributed HPC/HPN**
   - **for both open and less-open collaboration**
   - **within individual sites and across the enterprise**
2. **Design and Build Security into Systems**
3. **Develop Evaluation Criteria for Cyber Products**
4. **Develop Metrics of Success for CyberSecurity Programs**
5. **Develop policies and technolgies that consider the human factor**
6. **Utilize Test Beds**

Open Discussion

DOE scientific programs require cybersecurity policies –

these motivate a Technological response.

Some Technologies –

we can and will just buy and use.

Other DOE Requirements motivate DOE R&D, as

- **we need them earlier than general community**
- **we have unique requirements (HPC, HPN, distributed resources and scientists)**
- **as good citizens, we must contribute to the Internet community**